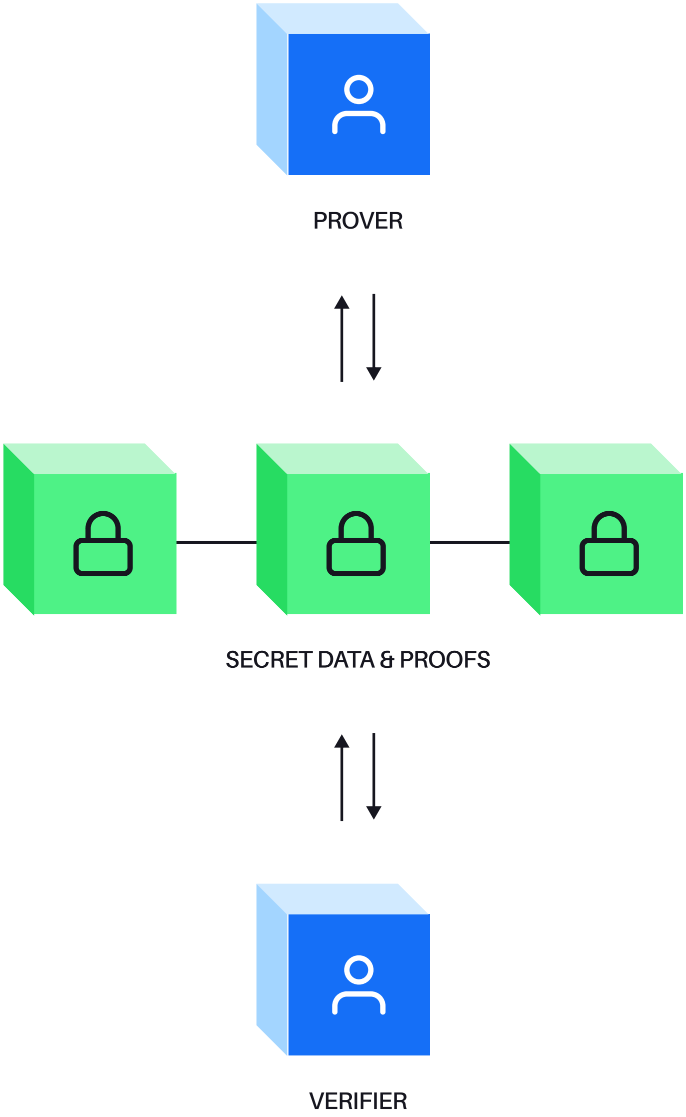
The Future of ZK Proofs



Protocol Labs

November 2023

Table Of Contents

01. Introduction

In a digital age rife with data breaches and online vulnerabilities, building trust is more crucial than ever. Zero knowledge proofs (zk proofs) offer an elegant solution beyond traditional privacy measures by allowing one party to verify certain information without ever disclosing the information itself.

Experts say zk proofs have the potential to revolutionize various industries, from finance and healthcare to luxury fashion and decentralized systems like blockchain, ushering in a new era of security and assurance. Independent research shows that zk proof generation will become a $10 billion market by the year 2030. Web3 services will require almost 90 billion zk proofs to be performed in 2030, with market-wide completion of 83,000 transactions per second.

This report will cover some familiar zk proof territory, including the differences between zk-STARKs and zk-SNARKs, a timeline of innovations in this space, challenges and future projections. The focus, however, is today's exciting inflection point where zk proofs are moving from research projects to serious business - an analysis derived from new and firsthand accounts from leading companies within the ecosystem of 250+ companies that form the Protocol Labs innovation network. With a shared mission to shape the future of computing, PL companies — including CryptoNet, Gensyn, Ingonyama, Lurk Lab, Polybase, Rarimo, StarkWare, Zama — have contributed to the world of zk proofs for years and will share their exclusive insights in this report.

Companies like Lurk Lab zero in on the complex mathematical models that form the basis of zk proofs. They believe the zk proof space is poised for growth:

“There’s been a decade of work to improve zk protocols that are leading to real business – we’re even seeing boutique venture capital firms that exclusively invest in this space. We are at an inflection point of better technology and more capital moving towards zk proofs," said John Burnham, co-founder of Lurk Lab. "It’s a Cambrian explosion.”

This report features exclusive research and expert commentary on the properties of zk proofs, use cases, challenges, potential disruptors, signs of momentum and future outlook.

INGONYAMA

Ingonyama, a PL network team that solves for hardware limitations by building semi-conductors to accelerate zk-SNARKs, stresses the importance of privacy in the next iteration of the internet:

ELAN NEIGER, HEAD OF MARKETING, INGONYAMA

“Information is the most valuable currency in the world. Yet we are all guilty of oversharing our data to third parties on the internet. Today if you want to prove one aspect of yourself, such as age, you must upload an ID which contains so much extra information — full name, address, country of citizenship, etc. What happens to that data? Often we find it's been leaked or stolen. This scenario happens every day in the digital world. The problem of oversharing can be solved by zk proofs, which are the most powerful cryptography that exists today for hiding data, while allowing for assertions on that data. ZK proofs are considered one of the greatest achievements of cryptography in the last 50 years.”

02.
What are Zero-Knowledge Proofs?

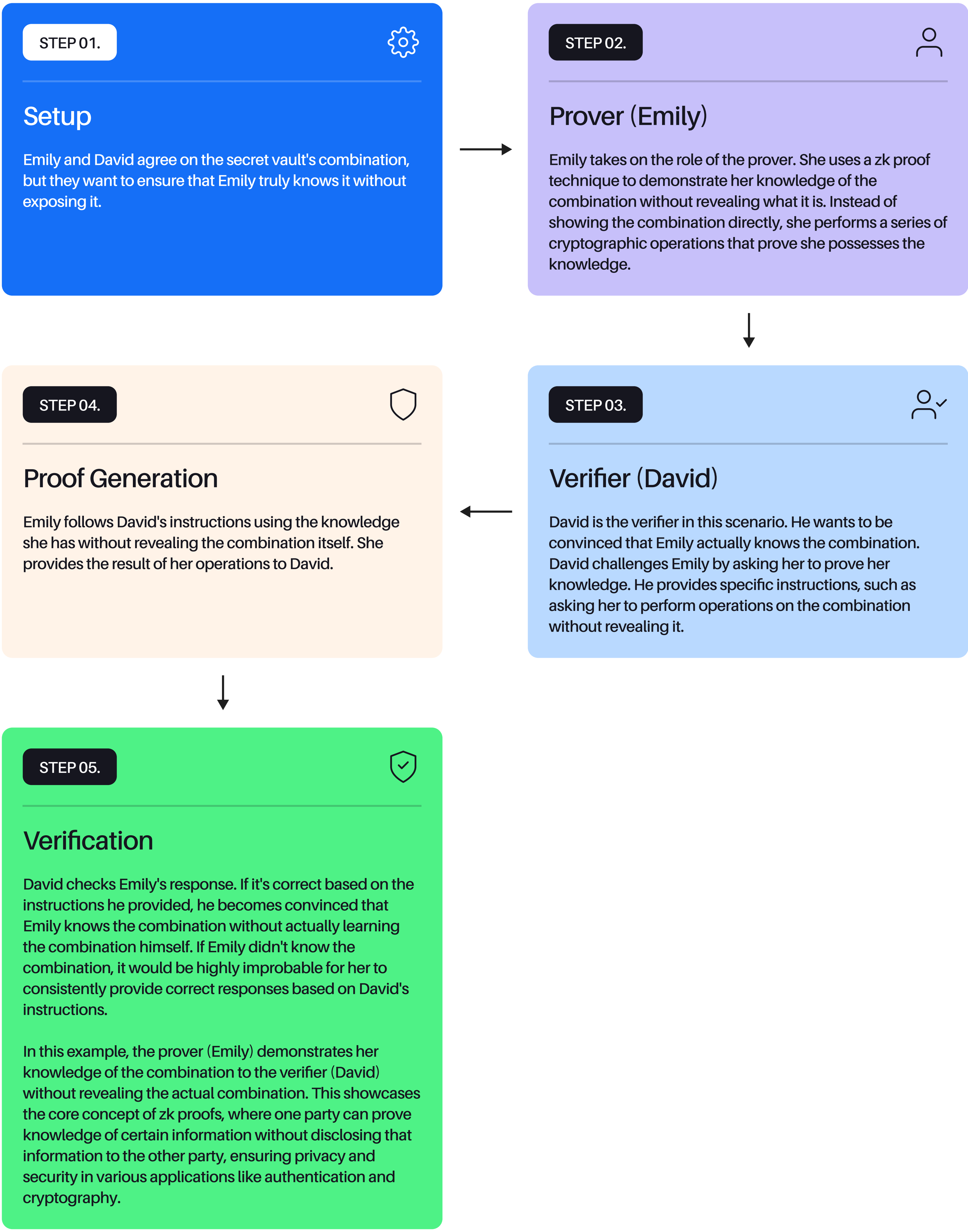
Picture this:

You're driving in an upscale neighborhood and spot the perfect house. You dial the realtor's number, ready to hear the asking price. What if there was a way to prove to the realtor right away that you're good for the money — no matter the cost — without revealing the total amount in your bank account? You could maintain your financial privacy and put in an offer right away.

Here enters the concept of a zero knowledge proof (zk proof). In this scenario, you present a zk proof to confirm you have enough funds for the down payment without revealing your entire bank balance or personal wealth. By establishing trust without unnecessary disclosures, zk proofs find practical application in various daily scenarios — ensuring secure digital transactions, verifying identity without exposing sensitive data, and revolutionizing privacy in the digital age.

In 1985, Shafi Goldwasser, Silvio Micali, and Charles Rackoff first introduced the concept of zk proofs to the world. Years later, one of their mentees, Rosario Gennaro, a researcher and former data scientist at Protocol Labs, wrote a highly cited paper about more efficient, publicly verifiable computer schemes that is still relied on today. He shares an example of a zk proof with a technical explanation here:

Step by Step Example of a ZK Proof



STEP 01.

Setup

Emily and David agree on the secret vault's combination, but they want to ensure that Emily truly knows it without exposing it.

STEP 02.

Prover (Emily)

Emily takes on the role of the prover. She uses a zk proof technique to demonstrate her knowledge of the combination without revealing what it is. Instead of showing the combination directly, she performs a series of cryptographic operations that prove she possesses the knowledge.

STEP 03.

Verifier (David)

David is the verifier in this scenario. He wants to be convinced that Emily actually knows the combination. David challenges Emily by asking her to prove her knowledge. He provides specific instructions, such as asking her to perform operations on the combination without revealing it.

STEP 04.

Proof Generation

Emily follows David's instructions using the knowledge she has without revealing the combination itself. She provides the result of her operations to David.

STEP 05.

Verification

David checks Emily's response. If it's correct based on the instructions he provided, he becomes convinced that Emily knows the combination without actually learning the combination himself. If Emily didn't know the combination, it would be highly improbable for her to consistently provide correct responses based on David's instructions.

In this example, the prover (Emily) demonstrates her knowledge of the combination to the verifier (David) without revealing the actual combination. This showcases the core concept of zk proofs, where one party can prove knowledge of certain information without disclosing that information to the other party, ensuring privacy and security in various applications like authentication and cryptography.

03.
A Timeline of Innovations

1985

Shafi Goldwasser, Silvio Micali, and Charles Rackoff introduce the concept of zk proofs in an academic paper, laying the foundation for the field.

1992

Oded Goldreich, Silvio Micali, and Charles Rackoff develop the concept of interactive zk proofs, where the verifier can interact with the prover to increase confidence in the proof.

2001

Fiat-Shamir heuristic is introduced as a technique to transform interactive zk proofs into non-interactive ones, making practical implementations more efficient and widely applicable.

2002

Jan Camenisch and Markus Stadler introduce the concept of group signatures with efficient zk proofs, allowing members of a group to anonymously sign messages while maintaining the integrity of the group.

2009

Matthew D. Green, Ian Miers, Christina Garman, and Aviel D. Rubin propose Zerocoin as a cryptographic extension to Bitcoin, aiming to provide enhanced privacy using zk proofs.

2012

Computer scientist Eli Ben-Sasson announces the concept of zk-SNARKs.

2014

Zcash, a privacy-focused cryptocurrency, adopts zk-SNARKs to enable private transactions.

2018

The Zcash Foundation releases the Sapling protocol, which uses zk-SNARKs to provide stronger privacy guarantees for Zcash transactions.

2019

The zk-SNARKs project releases Halo, a new zk-SNARKs system that is more efficient and scalable than previous systems.

2020

Filecoin mainnet launches as a decentralized storage network and cryptocurrency. Filecoin is currently the largest deployed zk-SNARK to date. By 2023, the Filecoin network produces 6-7 million zk-SNARK proofs daily, each proof encompassing over 100 million arithmetic constraints.

2021

The Ethereum Foundation announces the launch of the zkEVM project, which aims to bring zk proofs to the Ethereum blockchain.

2021

zkSync, a layer-2 scaling solution for Ethereum using zk rollups, gains attention.

2021

Cairo, a programming language for zk-SNARKs, is introduced by StarkWare, simplifying the development of zk-rollup solutions.

2022

The zkSync project releases zkSync 2.0, a new zk rollup that is designed to be more efficient and scalable than previous zk rollups.

A NOTE ON ZK-SNARKS VS ZK-STARKS

Two cryptographic techniques, created in tandem, fall under the umbrella of zk proofs: zk-SNARKs and zk-STARKs. Both aim to achieve similar goals of proving the validity of statements without revealing the underlying data, but they differ in their underlying mechanisms and use cases.

- zk-SNARK is a type of zk proof that allows a prover to demonstrate the truth of a statement to a verifier in a succinct and non-interactive manner. It's particularly associated with privacy-preserving transactions in blockchain and cryptocurrency systems, like Zcash.

- zk-STARK is another type of zk proof that also allows for proving the validity of statements without revealing the underlying data. Though it requires interaction, it achieves better security by removing the need for trusted setups, unlike zk-SNARKs.

For details on zk-SNARKS vs zk-STARKS, read this piece by PL network team Consensys.

04.
Current Major Use Cases

ZK proofs have found diverse applications across various fields due to their unique ability to verify information without revealing the underlying data. Here are five major use cases:

Voting Systems

In a zk proof-based voting system, voters can prove that their vote is valid without revealing the actual choice they made. This maintains the secrecy of individual votes, while ensuring that the total count is accurate. Similar to the way they are used today by DAOs, zk proofs can be used to verify properties of the election process, such as the absence of double voting or the integrity of the tally, without revealing specific voter information.

Cryptocurrencies

Zcash may be the most notable cryptocurrency dedicated to preserving privacy - and zk proofs play a crucial role. They enable confidential transactions where the sender, receiver, and transaction amounts are hidden, while still ensuring the validity of transactions. ZK proofs can also verify the correctness of smart contracts without revealing the underlying data.

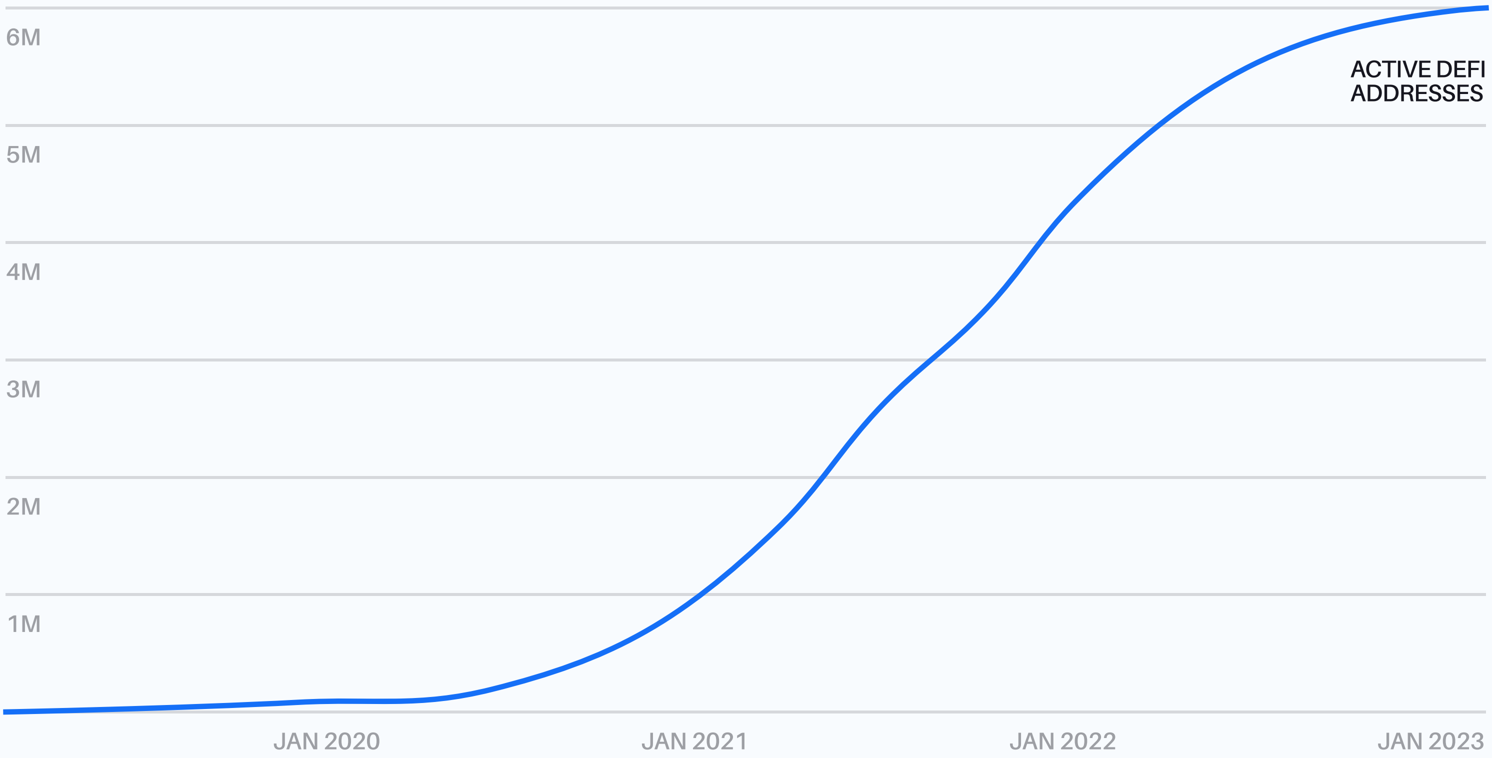
Decentralized Finance (DeFi)

Research shows that the DeFi market is growing rapidly and consistently, nearly doubling each year since 2018. According to data, the market is set to reach $67.4 billion by 2026. This translates to corresponding growth in the zk proof space, as DeFi platforms leverage zk proofs to enhance privacy and scalability.

ZK proofs are used to validate transactions and operations off-chain, while providing cryptographic proof of their correctness on-chain. This reduces the computational load on the blockchain and speeds up transaction processing. ZK proofs can also be used in decentralized exchanges to prove that users possess the necessary funds for trading without disclosing their exact balances.

Since 2019, when DeFi was relatively new, its quarter-on-quarter growth has risen at a rapid rate, with over 6 million unique wallets completing an on-chain transaction each month since late-2022.

NUMBER OF ACTIVE DEFI USERS



Data: Statista
Source: Finder's DeFi Statistics 2023

Supply Chain Transparency and Traceability

ZK proofs can be used to verify and authenticate the origin, movement, and authenticity of products within a supply chain without revealing sensitive proprietary information. This can enhance transparency by allowing different entities to independently verify the accuracy of claims made about products, such as their source, quality, and journey through the supply chain. For example, zk proofs could be employed to prove that a product was ethically sourced, without disclosing proprietary supplier data.

Environmental Standards

ZK proofs can be applied to verify compliance with environmental standards without revealing sensitive business data. For instance, companies can demonstrate that they meet certain emissions reduction targets without sharing specific emission levels or proprietary information. This aids in maintaining transparency and accountability while protecting sensitive information.

Polybase

Powered by zk proofs, Polybase is a layer 2 blockchain with private transactions and MEV-resistance. A member of the PL innovation network, Polybase's co-founder Sid Gandhi shares an example of an energy use case in the real world.

SID GANDHI, CO-FOUNDER OF POLYBASE

"One of the largest European energy companies wants to offer transparent data around renewable energy generation. Rather than quarterly manual audits, we look at real time data being generated from renewable resources. What percentage of the energy generated and sent to this particular client is green? Doing that in a cryptographically verifiable way isn't really possible. Consider data centers that don't want to reveal second-by-second energy data that they are consuming – that can be used for competitive intelligence.

What we allow with zk is the ability to keep that private data private, but then prove some public attributes of that data. So we could prove points like: what percentage of the data generated at this particular time is renewable? That's a very motivating use case for us, because that solves a real problem in the real world that we've seen with real customers. It's really exciting for us to be able to tackle this problem."

05.
4 Exciting Bets in ZK Proofs

In the evolving landscape of zk proof technology, there are several projects and cutting-edge techniques that are pushing the boundaries of what's possible, with a primary focus on enhancing efficiency, scalability, and usability. These innovative efforts are not only shaping the future of zk proofs, but also working towards broader adoption across various domains.

As these projects continue to mature and gain traction, the potential for zk proofs to revolutionize industries beyond cryptocurrency becomes increasingly evident, offering a promising future where privacy and security are paramount in our digital interactions.

Research shows that:

- The zk proof market is projected to reach $75 million in revenue in 2024
- Has the potential to exceed $10 billion in revenue by the year 2030
- Web3 applications alone are expected to require almost 90 billion zk proofs in 2030
- The average market clearing price per proof is expected to fall from $0.21 in 2024 to $0.12 by 2030

To that end, here are four big bets designed to increase adoption, including three top projects and one important technique that is helping build more efficient, scalable zk proof systems.

Source: Aligned.co, 2023

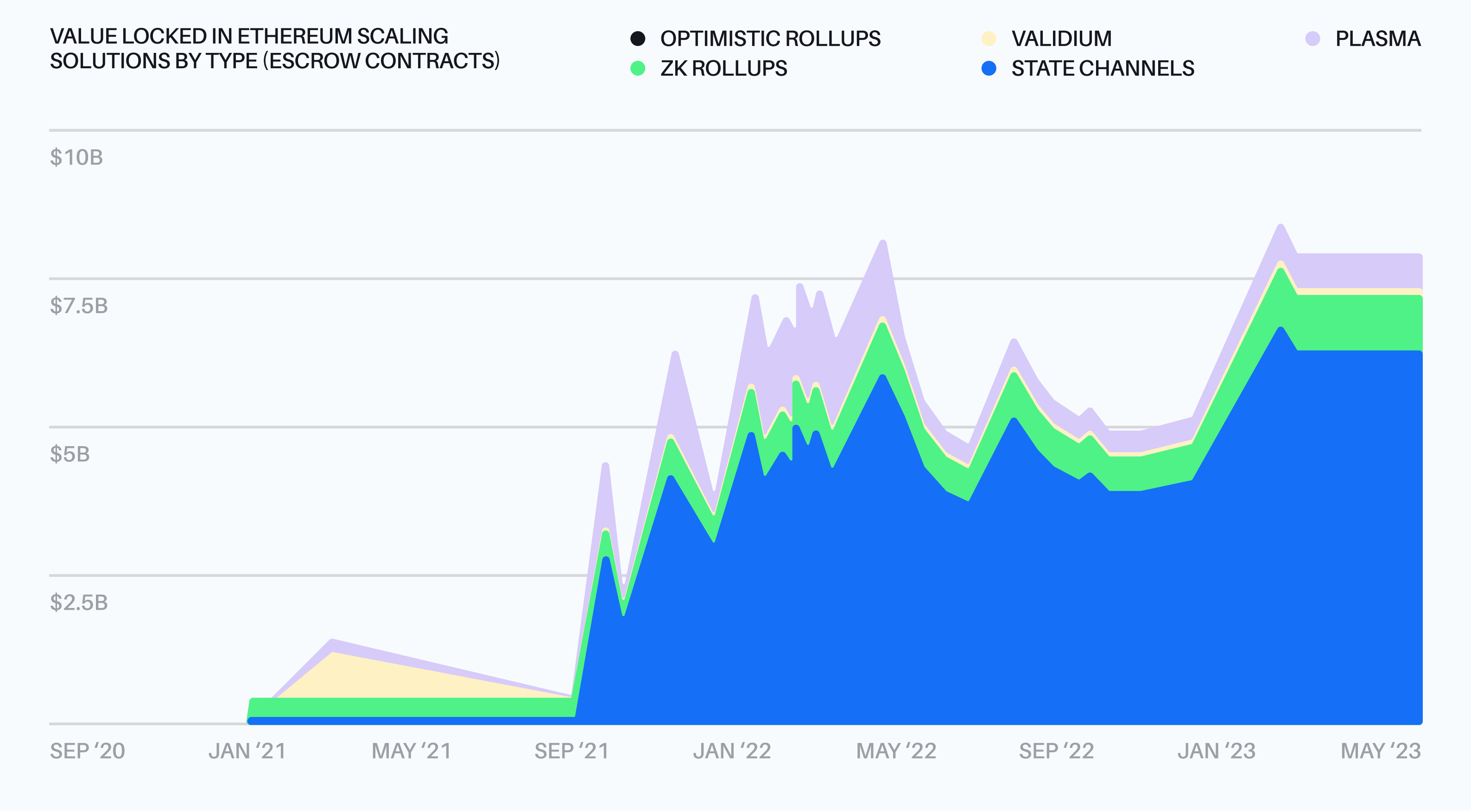
1 zkEVM

A concept within the Ethereum ecosystem aimed at developing a zk proof system that is compatible with the Ethereum Virtual Machine (EVM). It involves various stakeholders, including developers, researchers, and the Ethereum community. This would allow zk proofs to be used for a wide variety of Ethereum applications.

2 zkSync

A method and project focused on developing zk rollups, a type of layer 2 scaling solution for Ethereum. ZK rollups use zk proofs to bundle multiple transactions together, verify them off-chain, and then submit a single proof to the Ethereum mainnet. This significantly reduces the computational load on the Ethereum network and enhances its scalability. Examples:

- zkSync is also the name of a specific project that has been developed to implement this method. It is initiated and maintained by Matter Labs, a company focused on improving the scalability and usability of blockchain networks. The zkSync project includes the development of the zkSync protocol, smart contract infrastructure, and associated tools.
- Emerging zk rollups, such as zkSync Era, have witnessed a growth in their total value locked (TVL) surging to $668 million in June 30, 2023, according to Crypto.com. This signifies an impressive 660% increase from $88 million on April 1, 2023.
- Research shows that the Total Value Locked (TVM) in ZK rollups is currently over $7.5B to date. Mid-September 2021 saw all scaling solutions adoption, including zk rollups, skyrocket:



Source: The Block

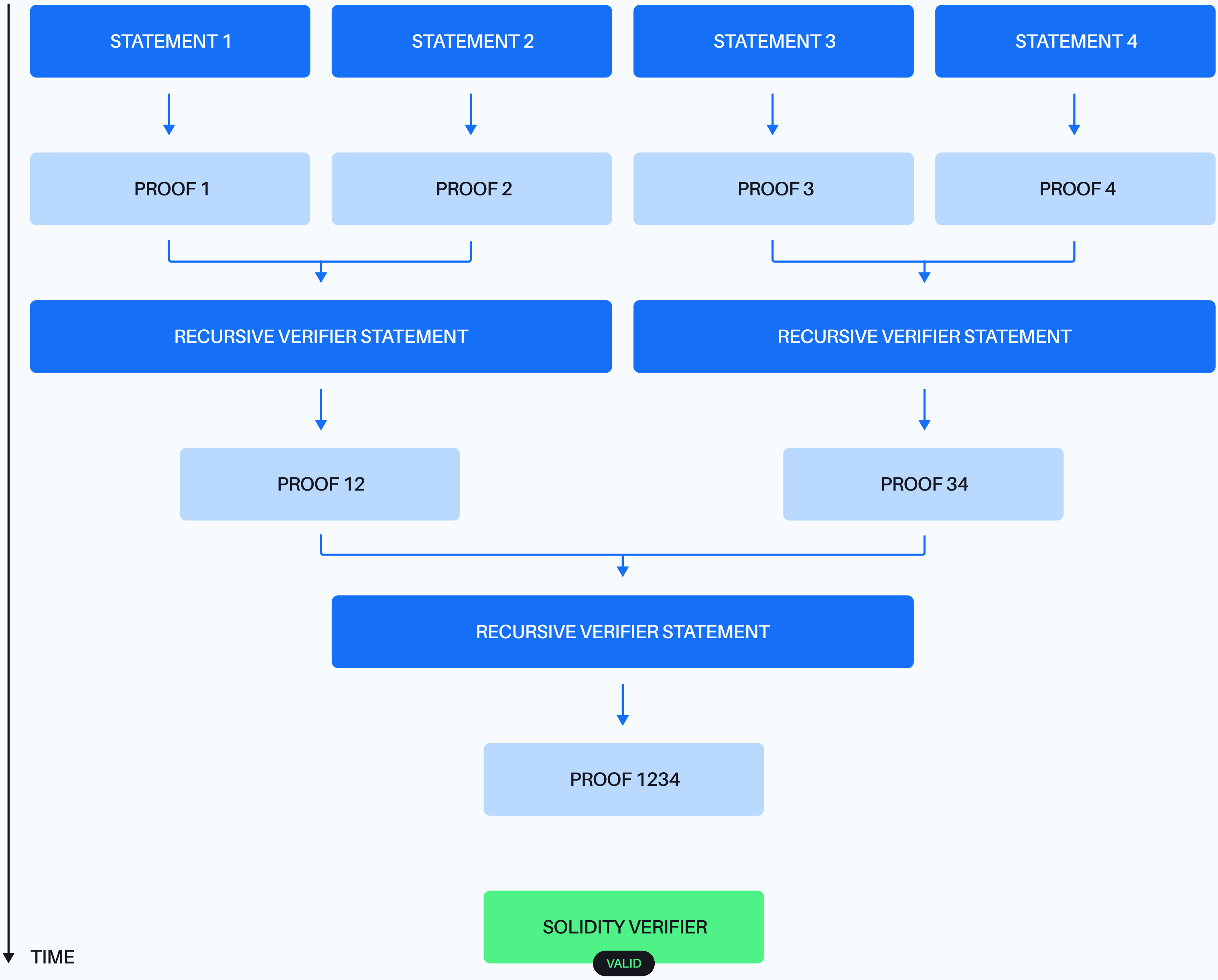
Updated: Aug 7, 2023

3 zk-STARKs

There's exciting development around this proof system that is even more efficient and scalable than previous systems. This could make zk proofs practical for a wider range of applications.

4 Recursive zk proofs

A technique that allows for the aggregation of multiple proofs into a single proof, drastically reducing the computational overhead of verification. This innovation has contributed to improved scalability in zk proof systems, making them more efficient for applications with a high transaction volume. Usually, the way it is used is in evolving computation: First, it breaks the computation to be proven into smaller steps and proves them iteratively. Each step contains a proof, proving the current state of the computation. Then, a new proof for the next step can be generated by using the current step and its proof recursively showing the correctness of all prior steps alltogether. The proof update does not require recomputing from the very first step as in a standard zk proof, and it is independent of the total length of the computation.



A TYPICAL RECURSIVE PROVING FLOW - FROM STARKWARE (VIA MEDIUM POST)

PL network team team StarkWare is a zk-STARK proof pioneer, bringing privacy to the blockchain with over $1 trillion of cumulative trading done to date. The team believes recursive proofs hold particular promise:

> “The benefits of recursion will be realized gradually, as it continues to allow for new improvements, and it will soon deliver hyper-scale, cut gas fees, and improve latency by unlocking the potential of parallelization. Further optimization of the Recursive Verifier is on-going and even better performance and cost benefits are expected to be provided over time.”

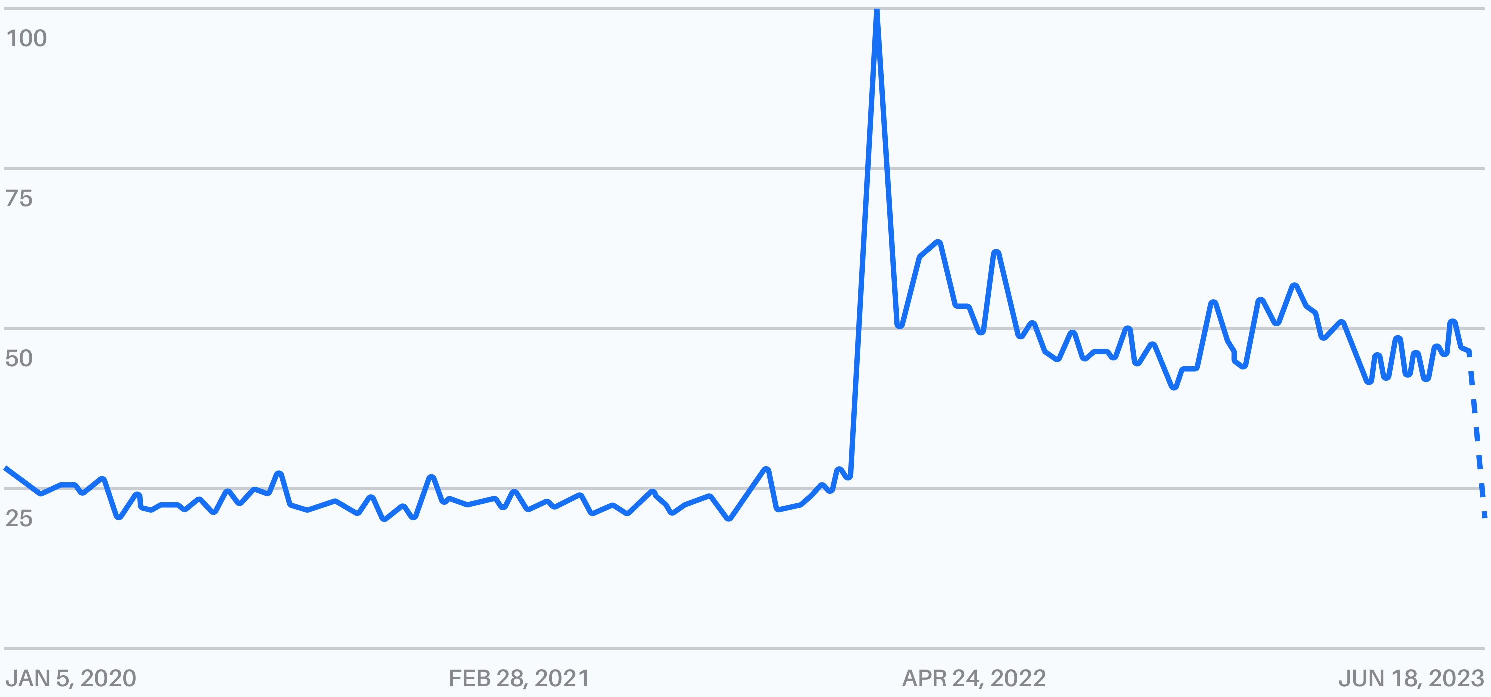
GIDI KAEMPFER, HEAD OF CORE ENGINEERING, STARKWARE

06. Signs of Momentum

1 Rising public interest

Following a series of key announcements in 2021 including the launch of Cairo, zkEVM and zkSync, there was a spike in Google Trends search for the term 'zero knowledge proof' in early 2022 that led to a sustained increase in interest.

INTEREST OVER TIME



RELATED SEARCH QUERIES:		
	1. ZK-SNARKS EXPLAINED	+160%
	2. ZKSYNC	+350%

SOCIAL MONITORING BY PL TEAM
TL;DR IN H1 OF 2023 ON ZK PROOFS:

NUMBER OF MENTIONS OF ZK PROOFS ON SOCIAL MEDIA IN H1 OF 2023

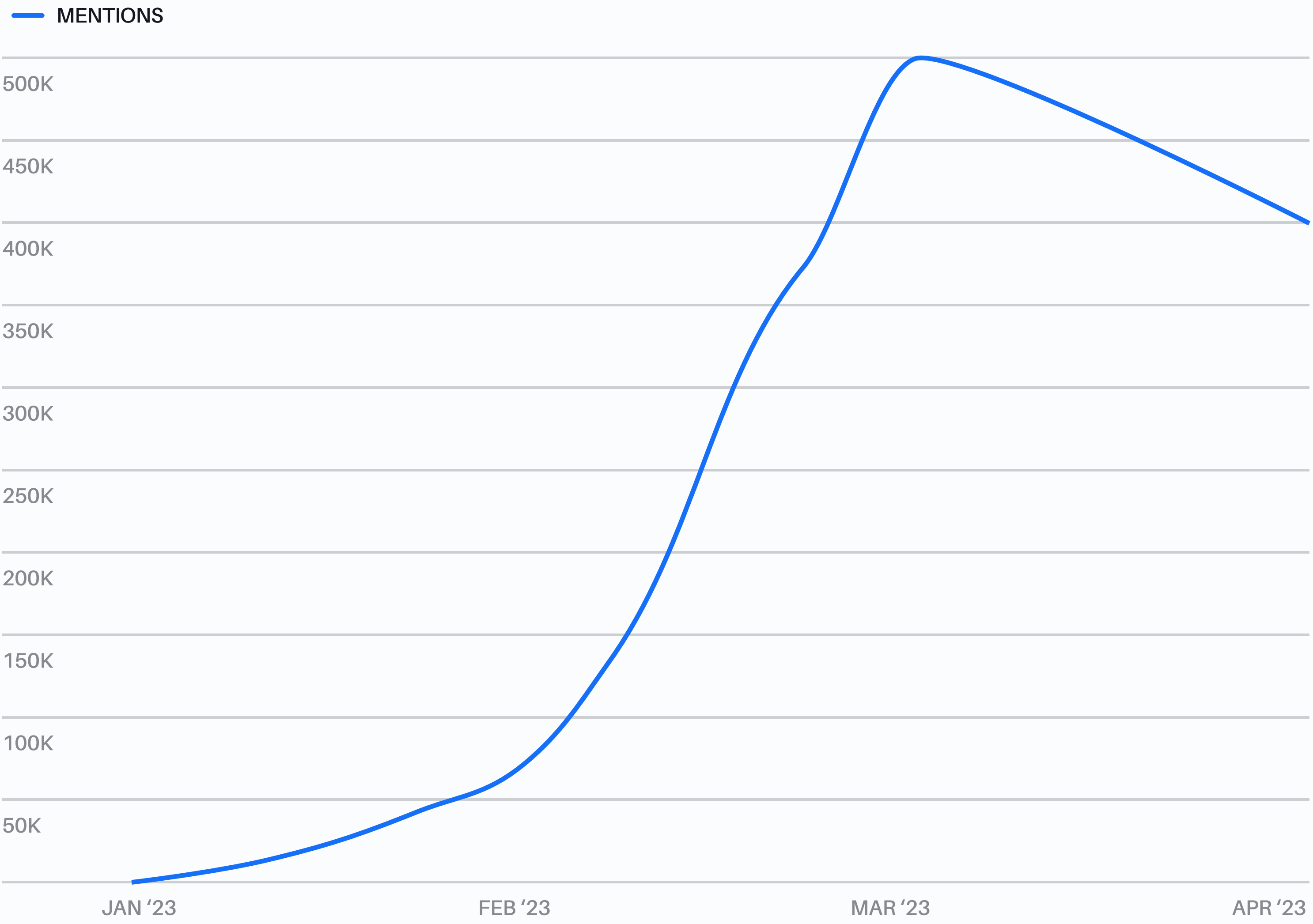
1.2M

MENTIONS

REACH OF THIS TOPIC IN H1 OF 2023

3.05B

REACH



ZK AS TOPIC REMAINS STRONGLY POSITIVE AND IS SLOWLY BECOMING ONE OF THE MOST CONVERSED TOPICS. (VS DAO 5.7M)

2 Increased funding by investors into the zk proof space

Zk Validator shows at least $725 million was raised by investors in 2022 alone

Polygon Capital raised $20 million in Jan 2022 for =nil; Foundation, an Ethereum development company dedicated to zk proofs, bringing its market valuation to $220 million

Aleo raised $200 million in a Series B funding round led by Andreessen Horowitz and Paradigm. Aleo is a zk rollup platform that aims to provide privacy and scalability for DeFi applicatons

Aztec raised $100 million in a Series B funding round led by Polychain Capital and Greenfield Partners. Aztec is a zk privacy protocol that is designed to be used by DeFi applications.

Matter Labs raised $200 million in a Series C funding round led by Multicoin Capital and FTX Ventures. Matter Labs is a zk proofs research and development company that is working on a veriety of projects, including zkEVM.

Lurk Lab is a Turing-complete programming language for recursive zk-SNARKs that will enable new possibilities for SNARK proofs, blockchain consensus, the Filecoin Virtual Machine (FVM), decentralized apps, data integration with IPFS and IPLD, and more.

JOHN BURNHAM, CO-FOUNDER OF LURK LAB.

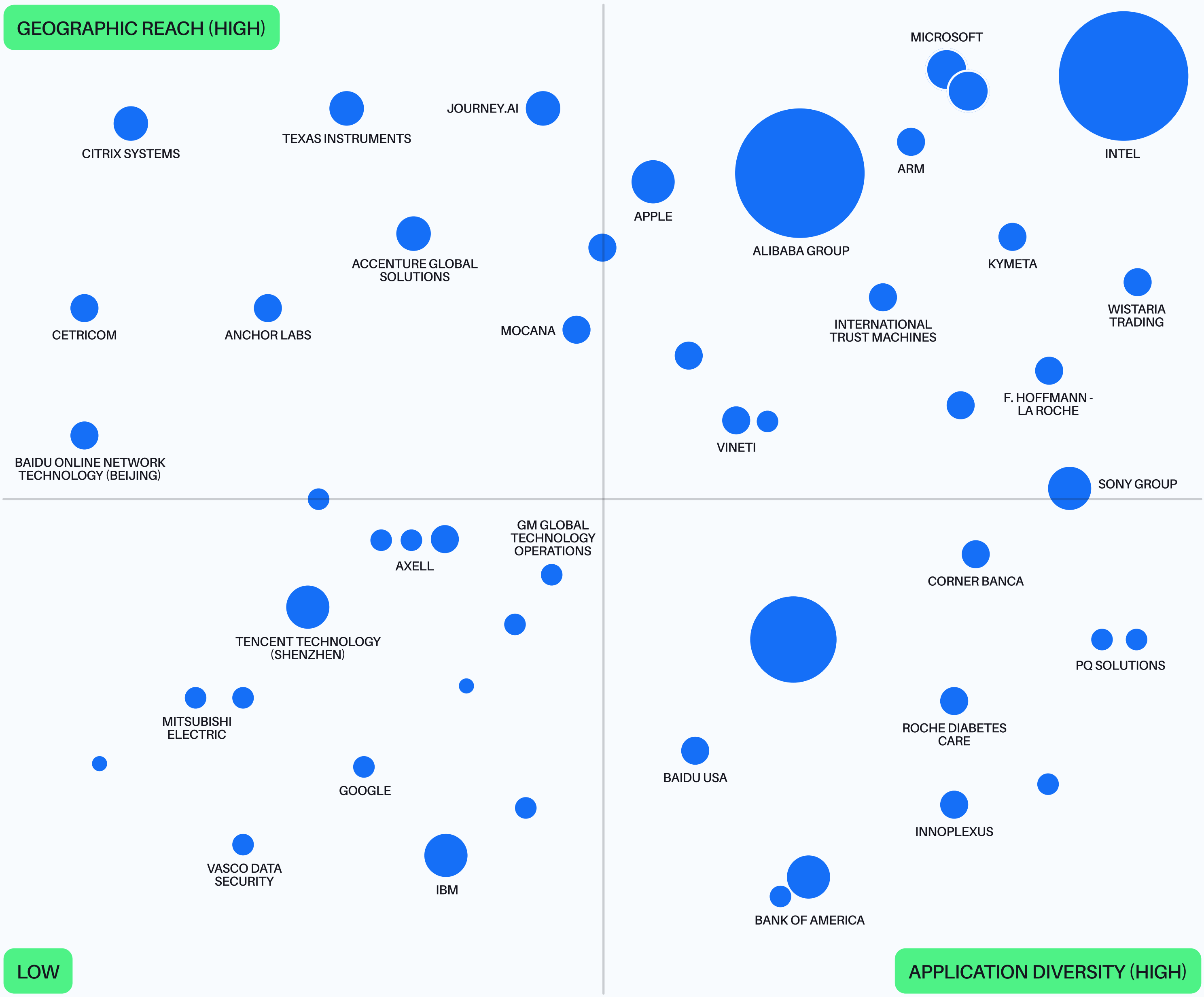
> “What's happening now is that the first generation of zk proof projects have led to a second generation of companies that have the potential to build huge businesses, multi-billion dollar valuation entities that rely on zk proofs. Investors have been much more willing to put capital into these zero knowledge projects and we’ve witnessed a new wave of them, like zk rollups and zkEVMs. “

3 Important legal patents filed

In the last three years, there have been over 3.6 million zk patents filed and granted in the technology industry, according to GlobalData's 2023 analysis.

According to GlobalData, there are over 620 companies currently operating in the zk proof space. Some of the biggest players in terms of patent filings to date include SoftBank Group, IBM and Macerich, depicted as the larger bubble sizes in this graph:

PATENT FILINGS IN THE ZK PROOF SPACE (2010-2021)



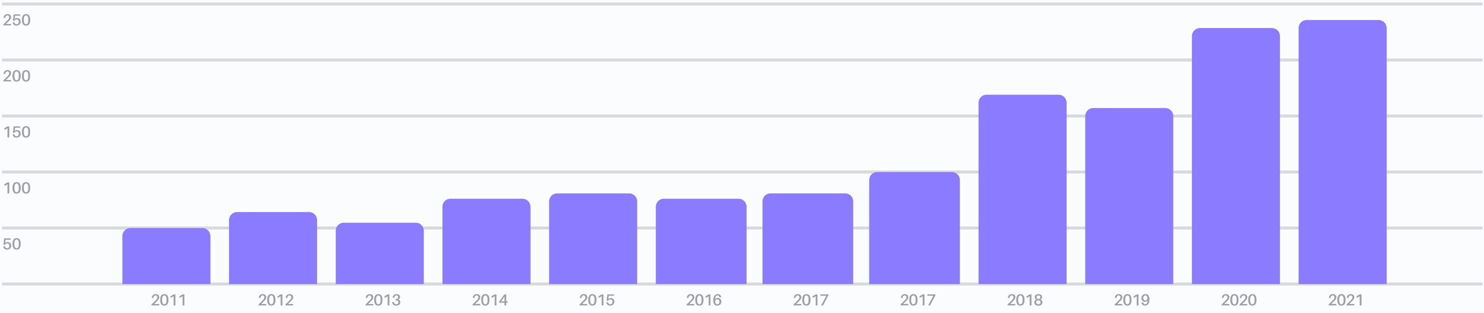
Bubble size = patent volumes between 2010 and 2021
Application diversity and geographic reach scores are normalised and ranked on a scale between 0 and 1
Source: GlobalData Patent Analytics

4 Increased developer adoption & rising opportunities (ZKML, ZK x AI)

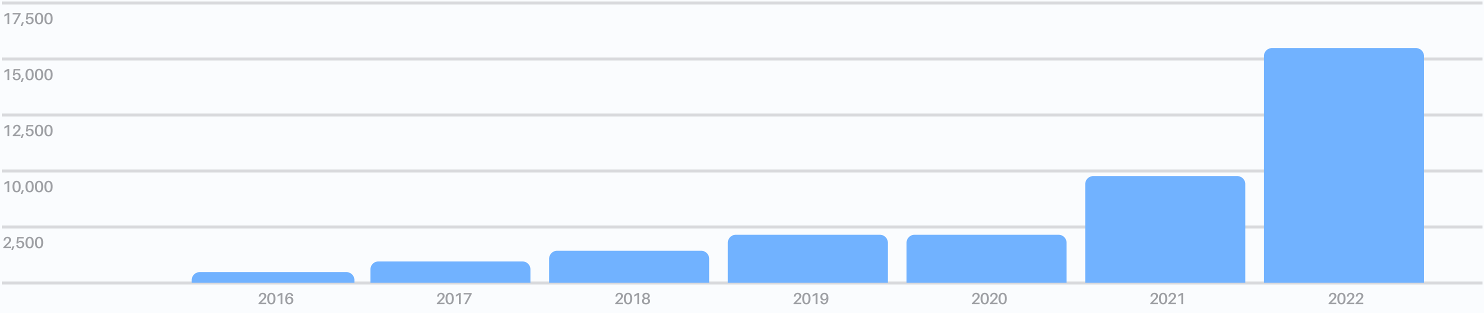
ZK-related research, developer adoption, and usage is on an upward trajectory. Data shows a particular increase in zkSync and zkEVM interest:

THE ZERO KNOWLEDGE FIELD IS GAINING MOMENTUM

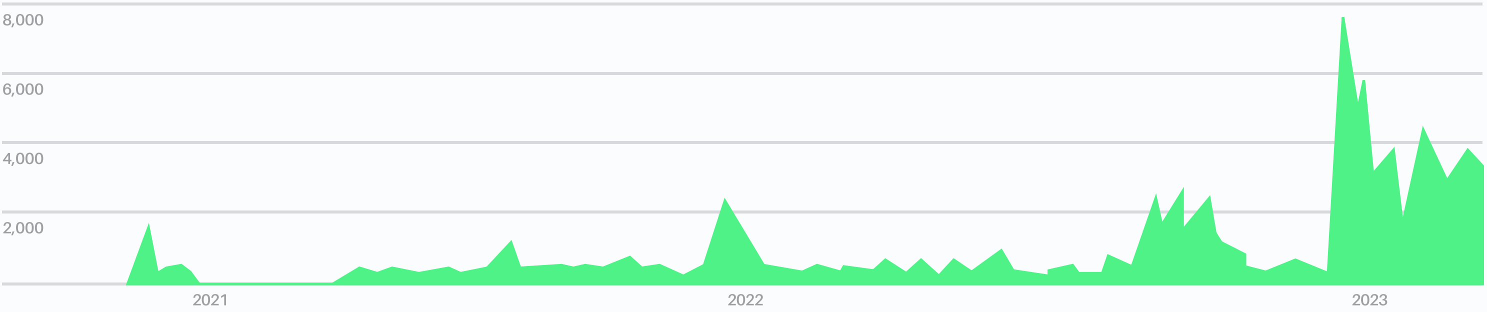
ZK-RELATED ACADEMIC PUBLICATIONS BY YEAR[1]



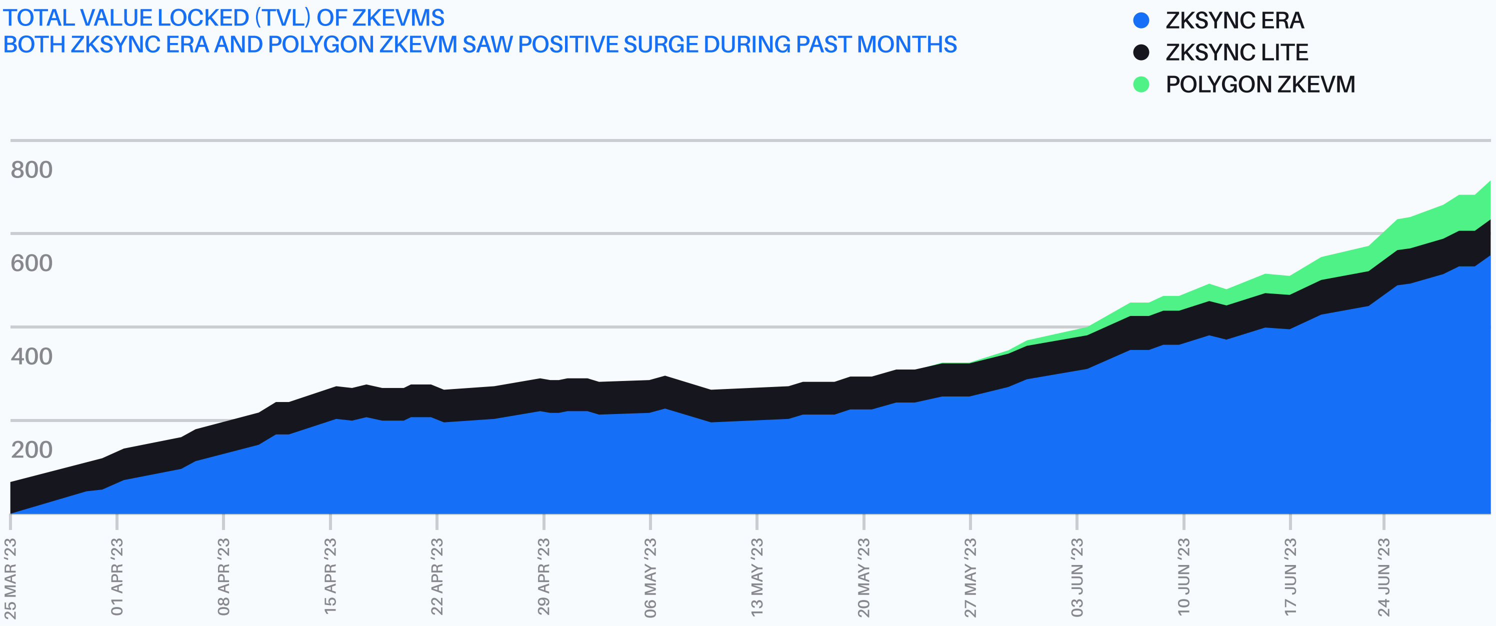
GITHUB STARS FOR KEY ZK REPOSITORIES[2]



DAILY TRANSACTIONS VERIFYING ZK PROOFS ON ETHEREUM[3]



Source: ZK repositories in Github: https://a16zcrypto.com/posts/article/state-of-crypto-report-2023/



TOTAL VALUE LOCKED (TVL) OF ZKEVMS
BOTH ZKSYNC ERA AND POLYGON ZKEVM SAW POSITIVE SURGE DURING PAST MONTHS

As of 28 Jun 2023
Sources: L2BEAT, Crypto.com Research

ZK x AI and Machine Learning (ZKML)

ZK proofs applied to machine learning, a sub-field of AI, hold particular promise. As AI-generated content becomes increasingly indistinguishable from human-created content, zero knowledge cryptography could be used to verify that a specific piece of content was produced by a specific LLM. This could be done by creating a zero knowledge circuit representation of the model, which would allow the content to be verified without revealing the model itself or any of the input data.

gensyn

Gensyn network is the L1 Machine Learning Compute Protocol that provides developers with ultra-low cost, P2P, access to all of the world's compute. The PL network team finds particular promise in the intersection of the ZK world and machine learning (ZKML).

HARRY GRIEVE, CO-FOUNDER OF GENSYN

"ZK proofs are different enough that it's hard to build a generalized market. The key takeaway here is the vertical specific applications; notably, in Zero Knowledge Machine Learning (ZKML) where it has two interesting use-cases: reducing compute verification overheads (e.g. for Machine Learning Compute Protocols like Gensyn), or proving that a given Machine Learning model has been applied (e.g. a fraud filter running on the Worldcoin hardware)."

PL network team Rarify Labs is a service provider and community member dedicated to advancing the next-generation interoperability protocol Rarimo. Rarimo focuses on the identity space, which is one of the most mature and promising markets for zk proofs.

KITTY HORLICK, DIRECTOR,
RARIFY LABS

"The zk proof market is highly promising and already moving towards tangible use cases. Identities are at the heart of the rapidly expanding decentralized social layer, including decentralized social media, DAOs, reputation systems, and on-chain gaming. Moreover, the use of zk proofs is accelerating due to the urgency with which identity credentials are needed both within Web3 and Web2 as AI-generated bots and deep-fakes make it increasingly difficult to discern humans – and human-generated content – from machines and AI-generated content."

07. Challenges & Hurdles

ZK proofs offer exciting possibilities for privacy, security, and efficiency. However, they also come with several technical challenges and adoption barriers for researchers, developers, and practitioners working in the realm of zk proofs. These multifaceted issues range from efficiency and scalability limitations to concerns about security assumptions and real world implications. By addressing these challenges, the cryptographic community can pave the way for the broader utilization of zk proofs in domains ranging from blockchain and cybersecurity to privacy-preserving technologies and beyond. Here are five challenges currently in focus:

1 Computational Complexity

Many zk proof systems involve the use of sophisticated cryptographic operations applied to a complex mathematical representation of a computer program. This complexity can make it challenging for developers to adopt and integrate zk proofs into their applications. It also affects the efficiency and scalability of large-scale zk systems.

> “The main challenge is around the balance of cost, time and proof size. This is the Holy Grail: to generate a proof with zero overhead and super small proof size. Now, we have achieved super small proof sizes, but with other big trade-offs. Generally the trade-off is: it becomes more expensive.”

NICOLA GRECO, RESEARCH SCIENTIST, CRYPTONET

2 Scalability

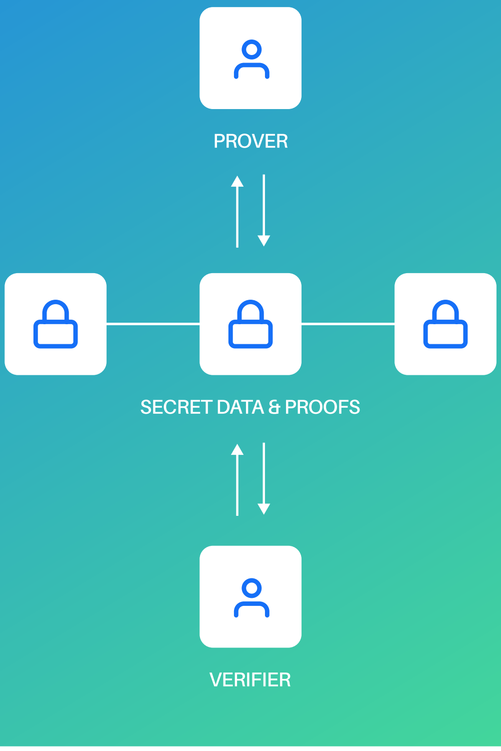
While zk proofs can aggregate multiple proofs and transactions, scalability challenges can arise when dealing with a high volume of transactions. Generating and verifying a large number of proofs may introduce bottlenecks. Achieving strong privacy guarantees through zk proofs might involve trade-offs in terms of transaction speed, network overhead, or computational load. Striking the right balance between privacy and performance is crucial.

Research scientist Rosario Gennaro explains that building a zk proof involves running a program that stores the state of the virtual machine at every step of the proof, making space a bottleneck to growth and speed of transaction. Folding schemes present a solution for proofs that are computed at every step of a computation: given a proof with correct computation up to, for example, step 4, the next correctness proof is obtain by "folding" the proof of correctness of step 5 into the previous proof, without the need to store the state of the computation at every stage.

Protocol Labs

ROSARIO GENNARO, PROFESSOR AT THE CITY UNIVERSITY OF NEW YORK

> “Instead of writing the entire transcript for the computation down at each step, folding compresses the computation and solves the space problem. There is a lot of work happening on implementing folding schemes to build efficient zk virtual machines, ranging from Web2 companies like Microsoft to cutting edge startups like Lurk Lab. While this bottleneck hasn’t been fully resolved, it’s one area where we are ahead of the curve to solve the issue and definitely an area to watch.”



3 Trusted Setup

Some zk proof systems require a trusted setup phase to generate initial parameters. The trusted setup phase requires that the individuals or entity responsible for generating these parameters act honestly and do not keep any secret information that could compromise the security of the system. If this setup is compromised or not performed correctly, it can undermine the security and privacy guarantees of the system. The field of zk proofs is rapidly evolving, with new advancements and potential vulnerabilities regularly emerging. Continuous research and development are essential to address security issues and improve the efficiency of zk proof systems.

4 Interoperability

Different zk proof systems might use distinct standards and protocols, making it challenging to achieve interoperability between different systems. Creating common standards would enhance compatibility and efforts are currently underway with the likes of The ZKProof Community. ZK proofs also often come with proof sizes that can be large, making them less efficient to transmit and store. Efforts to minimize proof size while maintaining security are ongoing. To support standardization, Polybase has released a new zk benchmark site, https://zkbench.dev/, with detailed comparison tables and open community reviews.

Polybase

SID GANDHI, CO-FOUNDER OF POLYBASE

“We're at that phase in the industry where people understand the high level capability, like keeping data private, proving things publicly, but there is still a big educational aspect around the trade-offs and the technical implementation, and, potentially, what other options are available, what trade-offs exist with those options as well. So, we are doing quite a bit of education. And then, the next step after that is selling our actual product. So it's a two-step process right now.”

5 Hardware Acceleration

Hardware acceleration techniques, such as using trusted execution environments (TEEs) or specialized hardware like ASICs, have enabled faster and more efficient computation of zk proofs. This breakthrough has the potential to make zk proofs practical for real-time applications.

INGONYAMA

ELAN NEIGER, HEAD OF MARKETING, INGONYAMA

"Today's hardware is not built for zero knowledge. ZK proofs require a massive amount of computational resources and existing hardware (CPUs, GPUs) are not designed to handle this computation efficiently. The main bottleneck is proof generation, which is still too slow and expensive. In terms of timing, zk algorithms have been developed for four decades, and zk software engineering for about 10 years. The missing ingredient is specialized hardware in order to accelerate proof generation, which is needed in order to commoditize the technology and make it accessible to everyone.

ZK proof generation must be an order of magnitude faster than it is today for real world use-cases. And that's what we're working on. Most of the demand today comes from the blockchain industry for scaling and privacy, but what makes me even more excited for zk proofs is the fact that once we get outside of the Web3 ecosystem, zk can impact nearly every industry, from medical research to AI, to decentralized ID, to new online multiplayer gaming architectures, and beyond."

08.
The Future of ZK Proofs

The industry is evolving at a rapid pace, with a focus on moving from research to a business-led model. On one hand, the near future is focused on addressing challenges and roadblocks in this space, which include hardware acceleration and faster computation. Here, PL network teams share their top three projections for the zk proof space in the near future.

1 Seamlessness

In the next 2-5 years, Rarify Labs expects an era of widespread integration of zk proofs across multiple protocols and technologies. Its presence will revolutionize privacy, digital identities, and blockchain performance, all while being seamless and mostly invisible to users, similar to the way SSL and secure enclaves in phones are invisible to users. ZK technology will have a user-centric flow that enables scaling and accessibility across the digital identity space.

ra

KITTY HORLICK, DIRECTOR,
RARIFY LABS

"ZK proofs will help dissolve the boundaries between Web2 and Web3, particularly within the identity space as it is currently the only technology that sits across both realms. More generally, zk proofs will massively reduce computation complexity and help deliver truly performant blockchains."

2 Client side integration

In the ever-evolving landscape of cryptography, Ingonyama believes zk proofs will transcend server-side applications and find their place within the very devices we carry in our pockets. Imagine the power of a world with zk proof hardware embedded directly in your mobile device, capable of running a proof of ownership or proof of personhood.

“We envision a future in which zk is not just running on the server side like data centers and cloud, but also on the client side – in mobile phones and gaming machines. ZK technology is fundamental to trustless compute. We're working to make efficient, zk proof hardware accelerators that can run everywhere.” said Elan Neiger, marketing lead at Ingonyama.

3 Cost efficient proofs

As zk proof methods evolve and proofs themselves become smaller in size and more cost effective, they will become an attractive option within the realm of the Internet of Things (IoT). Currently, IoT devices store all their data in centralized storage and data is stored directly onto their servers. ZK proofs allow for proofs to be used in place of stored data, creating efficiencies and cutting costs.

INGONYAMA

ELAN NEIGER, HEAD OF MARKETING, INGONYAMA

“Another focus for the future of zk lies with the Internet of Things (IoT). With zero knowledge, it will be possible to cut the costs of data storage, by sending proofs instead of data to confirm that specific stages or conditions have been met. Zero-Knowledge also allows for yes / no answers to complex questions involving data or sensitive personal information. For example: do you have enough money in your bank account to buy this car - Yes or no? ZK today is still a small market, but growing, because it is the most powerful cryptography that exists for hiding data, while allowing for assertions on that data.”

Education and standardization are key to the evolution of zk proofs. To that end, Ingonyama launched an open source community effort in August 2023: Ingopedia, a repo for all things zk for beginners and experts, ranging from video tutorials to academic research (link). Ingopedia has been widely cited as a good place to dive into the deep end of zero knowledge.

Potential Disruptors

As the industry evolves, researchers and developers are keeping an eye out for potential disruptors. These include quantum computers, homomorphic encryption and interdisciplinary innovations:

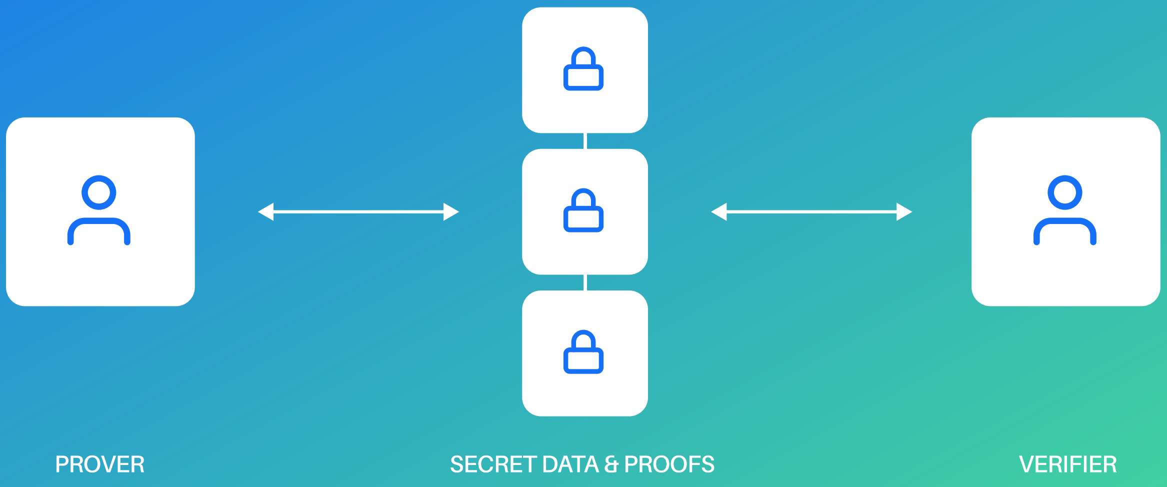
1 Quantum Computing

If large-scale, fault-tolerant quantum computers become a reality, they could potentially break certain cryptographic primitives that underpin zk proofs. However, should quantum computing become a reality, we will have to change all the deployed cryptographic schemes. There is already great progress with quantum-resistant encryption to date and industry leaders are making strides with quantum resistant SNARKs as well.

Protocol Labs

ROSARIO GENNARO, PROFESSOR AT THE CITY UNIVERSITY OF NEW YORK

> “All is not lost with the advent of quantum computing. In the future, we will see quantum resistant SNARKs. We know how to do quantum resistant encryption at this point. Should a quantum computer show up tomorrow, it will change everything. It won’t happen overnight, but we'll get there.”



2 Homomorphic Encryption

Fully homomorphic encryption (FHE) allows computations to be performed on encrypted data without the need to decrypt it. FHE and zk proofs serve different roles in cryptography, and their use cases often complement each other rather than disrupt each other. While FHE can be used for secure computation and privacy-preserving data analysis, zk proofs are typically employed for proving statements about data or knowledge without revealing that data or knowledge. However, if zk proofs over FHE computations were deployed, it could enable a new level of privacy-preserving computation, where not only the data, but also the operations performed on the data remain hidden. This would have significant implications for secure cloud computing, private data analysis, and more.

Actively building in this space, PL network team Zama is building an open source framework that enables developers to use homomorphic encryption to secure their Web2 and Web3 apps, without having to know cryptography. The homomorphic programs can then be deployed locally, to the cloud or to their upcoming decentralized infrastructure.

ZAMA

RAND HINDI, CO-FOUNDER OF ZAMA

“While zk’s strength is in verifiability, FHE focuses on privacy. When you combine the two together, you have the ideal solution, because you can have confidential computing that is actually verified. And so it's an area we’re very excited about. But zk has difficulty scaling existing tech. The way you implement zk is complicated, you have to resort to incredibly complex protocols. By contrast, FHE is just a smart contract running on-chain, like every other smart contract. But again, FHE cannot do what zk does, which is to prove that a computation is correct. This is why the future will likely see compatibility between the two, with zk for verifiability and FHE for privacy.”

3 Interdisciplinary Innovations

As the adoption of zk proofs expands, experts from various fields may come together to create novel applications and protocols. For example, collaborations between cryptographers, blockchain developers, AI researchers, and economists could lead to innovative solutions that we can't foresee yet. This cross-pollination of ideas might result in entirely new use cases and disruptive applications for zk proofs.

gensyn

HARRY GRIEVE, CO-FOUNDER OF GENSYN

> “Platforms will mature to the point where they’re ready for production use and then (hopefully) many applications will start appearing beyond the current under-the-hood/ scalability systems like zkEVMs or the current iteration of Starknet. We’re most excited about the applications in machine learning.”

RECOMMENDATIONS & ADVICE

Stay Updated with Research

Zero knowledge proofs is an evolving field with constant advancements. Stay updated with the latest research papers, conferences, and discussions in cryptography and related domains to remain informed about new techniques and developments.

Experiment and Prototype

Start by experimenting with existing zk proof libraries and tools. Creating prototypes will give you hands-on experience and help you grasp the practical aspects of using zk proofs. Collaborate with other researchers, developers, and experts in the field. It's a great way to learn the strengths and limitations of different zk proof systems.

Focus on Real-World Applications

While theoretical research is important, also consider practical applications. Think about how zk proofs can solve real-world problems like privacy-preserving data sharing, secure authentication, or improving blockchain scalability.

> "After many years, we finally have efficient proof schemes. By efficient, I mean that the prover time versus the normal computation time is getting closer and closer. The closer we get, the more we can have more applications that can be verified. In 2023, it's close enough to verify blockchain transactions. And maybe in the future, it can be closer to verify any computation."

NICOLA GRECO, RESEARCH SCIENTIST, CRYPTONET

FURTHER READING

ALIGNED RESEARCH
CONSENSYS: INTRODUCTION TO ZK-SNARKS
INGOPEDIA
ZERO KNOWLEDGE PROOFS: ETHEREUM.ORG
ZKPROOF STANDARDS

09. Appendix

THANK YOU TO THE FOLLOWING TEAMS AND PEOPLE WHO SHARED THEIR EXPERTISE:

PL NETWORK TEAMS FEATURED:

CRYPTONET – DATA SCIENTIST NICOLA GRECO & FORMER RESEARCH SCIENTIST ROSARIO GENNARO

CryptoNet is a community of researchers and engineers working on designing, proving and improving the building blocks for crypto-networks to engender new capabilities across the Web 3.0 stack.

GENSYN – CO-FOUNDER HARRY GRIEVE

The Gensyn network is the Machine Learning Compute Protocol that unites all of the world's compute into a global supercluster, accessible by anyone at any time, sharply lowering the cost of compute.

INGONYAMA – HEAD OF MARKETING ELAN NEIGER

Ingonyama builds semiconductors to accelerate a wide range of ZK protocols with an emphasis on zkSNARKs.

LURK LAB – CO-FOUNDER JOHN BURNHAM

Lurk is a Turing-complete programming language for recursive zkSNARK that will enable new possibilities for SNARK proofs, blockchain consensus, the Filecoin Virtual Machine (FVM), decentralized apps, data integration with IPFS and IPLD, and more.

POLYBASE – CO-FOUNDER & CEO SID GANDHI

Polybase is a public L2 blockchain with private transactions and MEV-resistance powered by zero knowledge proofs.

RARIFY LABS – DIRECTOR KITTY HORLICK

Rarify Labs is a service provider and community member dedicated to advancing the next-generation interoperability protocol Rarimo.

STARKWARE

A zkSNARK pioneer, StarkWare solves the inherent problems of blockchains – scalability and privacy.

ZAMA – FOUNDER AND CEO RAND HINDI

Zama is building an open source framework that enables developers to use homomorphic encryption to secure their Web2 and Web3 apps, without having to know cryptography.

REACH OUT:
CONNECT WITH THESE PROTOCOL LABS TEAMS TO COLLABORATE.

PROTOCOL LABS, SPACEPORT:
WRITTEN BY SARA HAMDAN

REVIEWED BY ANDREW WOO
& RICHARD CHANG

DESIGN, HOLOGRAPHIK:
LUKA PRIMORAC
FRANKO KOMLJENOVIĆ

GLOSSARY TERMS USED:

Recursive proofs: A type of proof that involves using a zk proof as a building block within another zk proof, allowing for more complex and layered privacy-preserving computations.

R1CS (Rank-1 Constraint System): This is a mathematical framework used to represent computations as a set of constraints, making it possible to construct zk proofs for a wide range of applications, including blockchain and privacy-preserving protocols.

Linear prover time: Refers to the desirable characteristic of zk proofs where the time it takes to generate a proof is directly proportional to the complexity of the computation being proven, making them efficient for practical use cases.

PlonK: A highly efficient zk proof system that stands for "Permutations over Lagrange-bases for oecumenical non-interactive arguments of knowledge," known for its scalability and performance in cryptographic applications.

zk-STARK: (Zero knowledge Scalable Transparent Arguments of Knowledge) is a type of zk proof that offer transparency and scalability while allowing one party to prove the knowledge of certain information without revealing that information itself.

zk-SNARK: (Zero knowledge Succinct Non-Interactive Argument of Knowledge) is a class of zk proofs that enable one party to prove to another that they possess certain information without revealing the information itself, while also being highly efficient and requiring minimal interaction.

Proof size: The amount of data required to represent and transmit a zk proof, which is a critical factor in assessing the efficiency and practicality of a zk proof system.

Verifier time: The computational effort required by a verifier to verify the validity of a zk proof, which is important for assessing the practicality and efficiency of a zk proof system.

ZKML: (Zero knowledge Machine Learning) is a concept that combines machine learning techniques with zk proofs to enable the training and utilization of machine learning models without exposing the underlying data used for training.

zkEVM: A concept within the Ethereum ecosystem aimed at developing a zk proof system that is compatible with the Ethereum Virtual Machine (EVM). It involves various stakeholders, including developers, researchers, and the Ethereum community. This would allow zk proofs to be used for a wide variety of Ethereum applications.

zkSync: A method and project focused on developing zk rollups, a type of layer 2 scaling solution for Ethereum. ZK rollups use zk proofs to bundle multiple transactions together, verify them off-chain, and then submit a single proof to the Ethereum mainnet. This significantly reduces the computational load on the Ethereum network and enhances its scalability.

ZK rollup: A type of Layer 2 scaling solution for Ethereum. zk rollups use zk proofs to bundle multiple transactions together, verify them off-chain, and then submit a single proof to the Ethereum mainnet.

Folding: A technique used to reduce the size and complexity of a zk proof, making it more efficient and practical for verification while preserving its security properties.